REMARKS

In the Specification

Three paragraphs were amended to correct minor typographical errors.

In the Claims

Rejection under 35 USC § 101

Claim 13 has been rejected under 35 USC § 101 because based on the position that the encrypted signal is merely "software," which is not tangible and thus not statutory subject matter.

While it is true that an encrypted signal may be formed from a non-encrypted signal using software, the resultant encrypted signal is certainly not "software." The encrypted signal is indeed a tangible (i.e., physical), regardless of whether it is electrical-based or light-based. It is well established in the patent laws that inventions involving the transformation of physical signals constitute statutory subject matter (see, e.g., *Arrhythmia Research Technology, Inc. v Corazonix Corp.*, 958 F.2d 1053, 22 USPQ 2d 1033 (Fed. Cir. 1992)).

The rejection of claim 13 on the basis of the encrypted signal constituting non-statutory subject matter is clearly erroneous as a matter of law, and the Assignee respectfully requests that this rejection be withdrawn.

2. Rejection based on nonstatutory obviousness-type double patenting.

The Examiner has rejected claims 1-13 under the doctrine of obviousness-type double patenting in view of the co-pending continuation-in-part (CIP) identified as patent application serial no. 10/837,775, which CIP is commonly owned along with the present Application by the above-identified Assignee, as evidenced by respective assignments recorded in the USTPO at Reel/Frame 015299/0423 and at Reel/Frame 014517/0452.

Included herewith is a ***Terminal Disclaimer*** that obviates the obviousness-type double-patenting rejection.

3. Rejection of claims 1-16 based on 35 USC § 103(a)

Claims1-8 and 10-15 were rejected under 35 USC § 103(a) as being unpatentable over USP 6,701,437 to Hoke et al. ("Hoke") in view of USP 7,068,790 to Elliott ("Elliott"). Claims 9, 10 and 16 were rejected under essentially the same bases, presumably in addition to general knowledge in the art as reflected by the Examiner's language that "..it would have been obvious..." in rejecting these claims.

Both Hoke and Elliott need to be read and understood as a whole in order to properly apply them to the claims of the present Application.

Hoke discloses a computer system for processing communications in a virtual private network (VPN). FIG. 1 of the present Application essentially describes the teaching of Hoke as it relates to the invention claimed in the Application. Hoke does not disclose or teach, suggest, or provide any motivation for using QKD techniques in combination with the VPN system. Hoke also does not disclose, teach or suggest the use of FIPS in connection with sending QKD-encrypted signals over the VPN.

Elliott discloses systems and methods for setting up a path in a QKD network. The invention of Elliot involves establishing paths through an optical network to a data distribution endpoint. The paths to the data distribution endpoint can be changed via optical switches if eavesdropping is discovered in the path originally used. There is no discussion of VPN-type communication in Elliott. In Elliot, the quantum keys are used to encrypt the data directly, as is normally done in QKD communication systems. Elliot does not disclose, teach or suggest anything even remotely related to FIPS standards. In fact, rather ironically, the network system disclosed by Elliot would not be FIPS certified.

The Examiner falls short of making a *prima facie* case for obviousness because combining Hoke and Elliott does not yield Assignee's claimed invention. Assignee's claimed invention is directed to a VPN-type communication system that uses both quantum (i.e., QKD-based) encryption that is not FIPS-certified in combination with classical encryption that is FIPS certified. This makes the system ***as a whole*** FIPS-certified while also providing ***QKD-based encryption***. Assignee respectfully submits that it is ***counterintuitive*** to include both ***classical*** encryption and ***quantum encryption*** in a ***single*** communication system to achieve a ***FIPS-certified*** system having quantum security. In fact, Assignee's claimed system represents (to the best of Assignee's knowledge) the ***first*** FIPS-certified QKD-based encryption system.

It appears that the Examiner is reading both Hoke and Elliott out of context and impermissibly selecting specific items in these references to piece together Assignee's claimed invention. Both Hoke and Elliott need to be read ***as a whole*** and in the context of Assignee's claimed invention. Keeping this critical point in mind, the person skilled in the art would not think to use Elliot, which relates to the switching of optical paths in an optical network that uses direct QKD encryption, as the basis for achieving FIPS-compliant QKD encryption. And Hoke simply does not address the issue of FIPS compliance in the context of QKD encryption. While the inventions of Hoke and Elliot both include lots of VPN and QKD-related equipment, that's about all they have in common with Assignee's invention. There is simply no nexus between the inventions of Hoke and Elliot that would lead one skilled in the art to try to achieve FIPS compliance of a QKD system via a classical encryption device.

An important point to understand about Assignee's claimed invention is that the classical encryption step does not add any significant additional security to the system. The high degree of security provided is due to the QKD system integrated therewith. Intertwining the classical and QKD encryption is actually a rather non-obvious way of "hiding" the QKD aspect of the encryption beneath the FIPS-certified classical encryption in a manner that maintains the FIPS certification while at the same time using QKD encryption.

Also critical to understanding why Assignee's claimed invention is non-obvious is to realize that the usual approach to obtaining FIPS certification for a QKD system would be to go through the rigorous process of getting the QKD system FIPS certified directly. However, since QKD is a relatively new technology, it could take many years for such certification to be obtained.

Assignee's claimed invention provides FIPS-certified quantum encryption immediately.

In support of this important point, attached hereto is an article by Samuel K. Moore from the March 2007 issue of *IEEE Spectrum* magazine, entitled "Commercializing quantum keys." The article address the main issues associated with commercializing quantum cryptography. The third column, second full paragraph (see highlighted text) makes the important observation that "[b]efore customers will accept a new encryptor, it must pass a certification process ***that can take two or three years***" (emphasis added). This is a direct quote is from SmartQuantum, Inc., a competitor of the Assignee. The passage goes on to say that "we do not have the knowledge to develop a fully certified classical encryption system." This is ***precisely*** the point the present invention seeks to address.

The second-to-last paragraph of the *IEEE spectrum* article (see highlighted text) states that the above-identified Assignee "is scheduled for certification by the U.S. National Institute of Standards and Technology in 2007." This accelerated certification-- as compared to the competition (who by their own admission has not figured out a way to obtain such certification sooner) –is made possible by Assignee's claimed invention.

Finally, the article also illustrates the key point that ***one cannot simply combine a classical cryptography system and a quantum cryptography system and obtain a FIPS-certified system***.

CONCLUSION

Applicant respectfully requests that the above amendments to the specification be entered. Also, in view of the above remarks, Assignee respectfully submits that the presently pending claims are in condition for allowance. Accordingly, a Notice of Allowance for the Application is earnestly requested.

Joseph E. Gortych (Reg. No. 41,791)

Date: **April 05, 2007**

Correspondence Address (Customer #53590)
Opticus IP Law, PLLC
7791 Alister Mackenzie Dr.
Sarasota, FL 34240

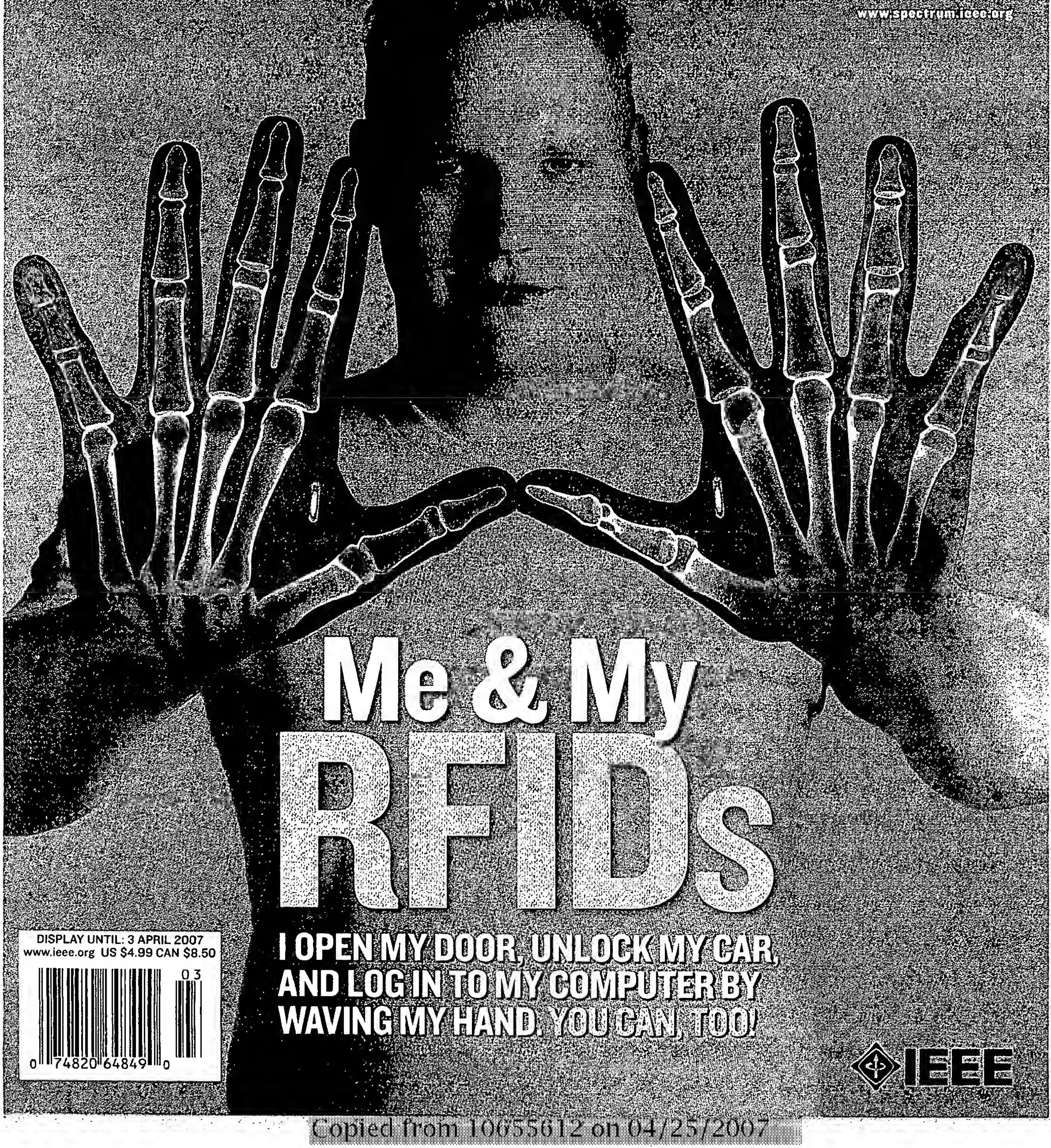
Telephone...941-378-2744
Fax...........321-256-5100
e-mail........jg@opticus-ip.com

REBUILDING NEW ORLEANS • AT&T'S FORGOTTEN TREASURES

IEEE SPECTRUM

THE MAGAZINE OF TECHNOLOGY INSIDERS

MARCH 2007
www.spectrum.ieee.org

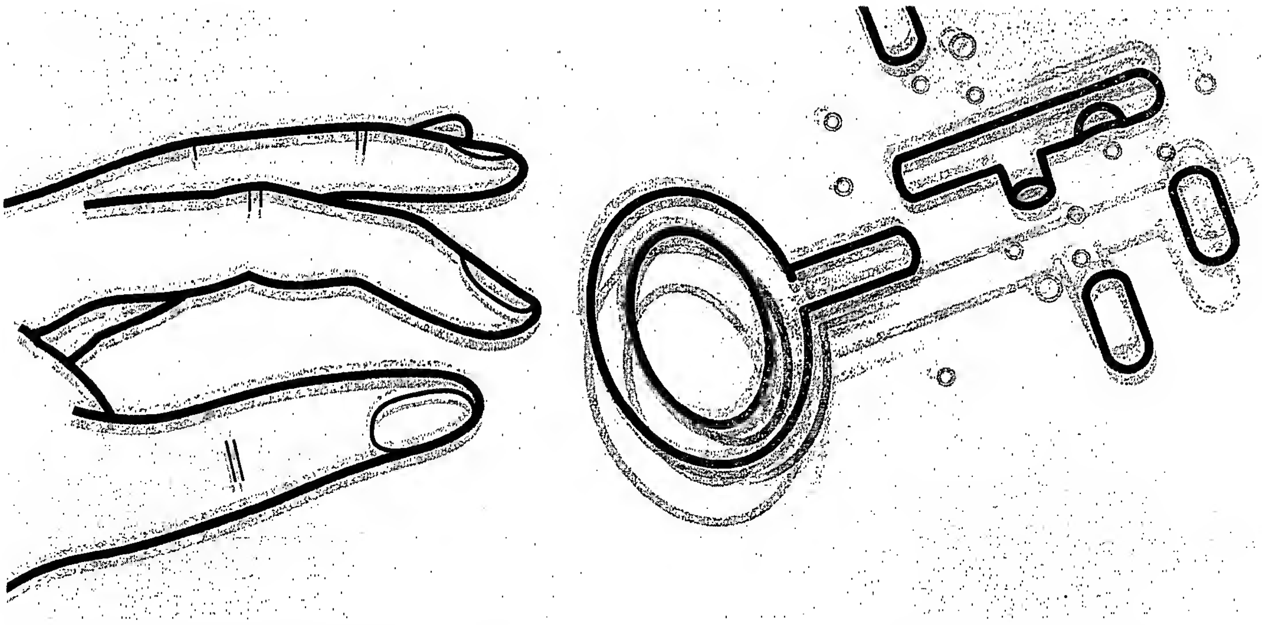


Me & My RFIDs

I OPEN MY DOOR, UNLOCK MY CAR, AND LOG IN TO MY COMPUTER BY WAVING MY HAND. YOU CAN, TOO!

DISPLAY UNTIL: 3 APRIL 2007
www.ieee.org US $4.99 CAN $8.50
03
0 74820 64849 0

IEEE



Commercializing Quantum Keys

Companies link spooky techniques to off-the-shelf distribution technology

It's a strange business, turning the esoteric quantum properties of light into money. But there are a few brave companies that have been trying to do just that for the last five years, and they may have hit on the right way to do it. What these firms, ID Quantique, MagiQ, and SmartQuantum, are trying to sell is a way of distributing a cryptographic key that is theoretically theft-proof, because it relies on the quirky quantum physics of photons. Such a "quantum key" distribution system could allow entities with secrets—banks, large technology firms, governments, and militaries—to encode and decode their data for transmission over optical fiber.

In the hopes of finally gaining customers, the companies involved have retooled their wares. Some are tying their quantum key distribution technology to high-bandwidth commercial devices that can use the keys to encrypt data. And some are looking to redesign their systems so that they can be integrated into telecom networks to make it more attractive for big carriers to offer quantum encrypted lines to their customers.

Quantum key distribution lets two computers generate a key between them by taking advantage of a quantum property of photons—the fact that a characteristic such as phase or polarization cannot be measured without changing it. A quantum key can be generated by transmitting a series of bits encoded using one or a few photons per bit and two types of polarization filters.

The bit the photon represents can be accurately read only by using the right filter. Use the wrong filter, and you change the bit. An interloper won't know which filter the encoder used even though the sender and receiver can share that information. So the would-be thief can't just insert himself between the sender and the receiver to read the bits, and any attempt he makes to do so will be easily noticed. Making it even more difficult for such data thieves, the systems these companies have developed commonly generate a new key about once a second.

ID Quantique, a spin-off of the University of Geneva, debuted the first commercial key distributor in 2002, followed quickly by MagiQ Technologies of New York City. By 2004 those two were joined by a French start-up, SmartQuantum, in Lannion. Big firms such as Mitsubishi, NEC, NTT, and Toshiba have been researching such systems as well.

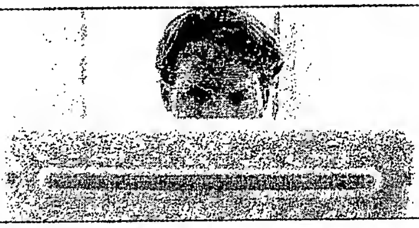
What customers really wanted, says ID Quantique CEO Grégoire Ribordy, was not just a key distributor but an integrated system that could both distribute the keys and do the data encryption at gigabit-per-second rates—a hybrid of quantum and classical encryption machines. All three firms initially focused on developing such devices in-house.

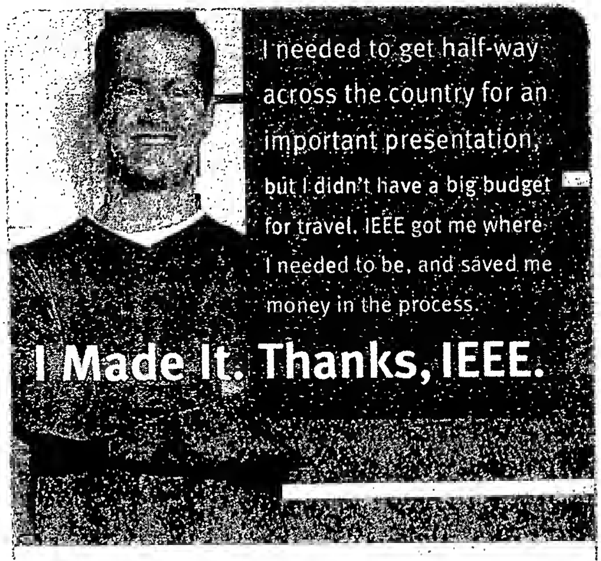
ID Quantique built a 100-megabit-per-second device that distributed keys on one fiber and transmitted encrypted data on a second, and MagiQ produced one that operates at 2 gigabits per second. Meanwhile, SmartQuantum built a 2-Gb/s device that did both the key distribution and the encrypted data transfer on the same fiber.

But it has proved too difficult for small start-ups to get such a system on the market quickly enough to compete with more established firms selling standard high-bandwidth encryptors. Before customers will accept a new encryptor, it must pass a certification process that can take two or three years, says SmartQuantum's commercialization and marketing director, François Guignot. "In the short term, we do not have the knowledge to develop a fully certified classical encryption system," he says.

So ID Quantique and SmartQuantum have shifted gears. Instead of focusing on building their own encryption systems, they are partnering with classical encryption providers to integrate quantum key distribution into established products. In January, ID Quantique announced an arrangement with Melbourne, Australia–based data security firm Senetas Corp. that gave birth to a 1-Gb/s hybrid. In a hybrid, a single key distributor can serve multiple encryptors. "When your bandwidth

JOHN DOMINIS/TIME & LIFE PICTURES/GETTY IMAGES
HARRY CAMPBELL



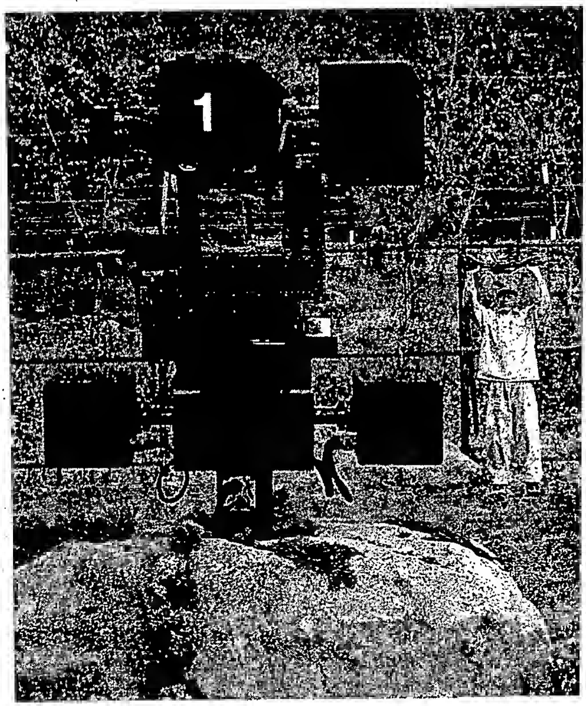


requirements grow, you can add 1-gigabit-per-second encryptors," says Ribordy. SmartQuantum is getting a similar integration project under way, using classical encryptors from two companies, which Guignot would not name.

For ID Quantique, integrating classical and quantum cryptography involved two steps. One was to develop a secure way of transferring the key from the quantum device to the classical one. The other was to come up with protocols for handling errors in the transmission and for synchronizing the two types of devices.

MagiQ, on the other hand, took a different path. It built its own integrated device through a partnership with Cavium Networks, in Mountain View, Calif., a maker of encryption/decryption microprocessors. Its 2-Gb/s product is scheduled for certification by the U.S. National Institute of Standards and Technology in 2007. And the company is pressing ahead on the bandwidth front, with an 8-Gb/s device due for production this month.

Even if their products are ready for the market, the market may not be ready for them. Banks, prime targets of ID Quantique, have only recently warmed to the idea of encrypt-



A Robotic Sentry For Korea's Demilitarized Zone

Go ahead, make its day.

A new gun-toting sentry robot, developed by Samsung Techw Co. for the South Korean government, may soon be coming a disputed border near you. The SGR-AI robot uses a low-lig camera and pattern recognition software to distinguish huma from animals or other objects and, if necessary, can fire its buil machine gun—a Daewoo K3.

ing their data while it's in transit, let alone using a new technology to do so.

Still, SmartQuantum's Guignot believes that there could be a €300 million market by 2009 for quantum cryptography companies, but only if they convince telecom providers to make sales for them. Say a bank wants to securely link its London and Paris offices. A telecom company would install hybrid encryptors within the telecom network. Then the provider could lease the bank a hybrid encryptor and an optical-fiber connection to the network, giving the bank essentially impenetrable encryption along the entire path. "This would be a premium product," says MagiQ CEO Robert Gelfond. He thinks providers could charge up to 30 percent more for a line like that.

The one hitch is that because commercial quantum key distribution works only over a maximum distance of 100 to 140 kilometers of fiber, the telecom provider might have to link several key distributors end to end within its network and guarantee that no one can gain access to the connection points. MagiQ has already taken the first step along this path. A year ago, it collaborated with U.S. carrier Verizon to demonstrate key distribution and data encryption over two linked 80-kilometer spans. **— SAMUEL K. MOORE**

Myung Ho Yoo, a principal research engineer at Samsung's Optics & Digital Imaging Division in Seongnam City, just southeast of Seoul, says the robot is the first of its kind to be commercialized. South Korea's need for such a robot is clear, he says. Unlike the border between the United States and Mexico or even those separating Israel from the occupied territories, the demilitarized zone that stretches for 250 kilometers between South and North Korea is patrolled along its entire length. With one guard post every 50 meters along the southern side, two guards per post, and twelve shifts per day, the man-years spent on guard duty quickly add up.

The Samsung robot packs a 5-millimeter, Korean-made light machine gun. Should it detect an intruder, "the ultimate decision about shooting should be made by a human, not the robot," says Yoo, who led the team that designed the robot. But the robot does have an automatic mode, in which it can make the decision.

The machine's real innovation is its color camera, which can pinpoint a target from up to 500 meters away in illumination down to 0.008 lux (lumens per square meter), about the same as a starlit night. The robot has three such cameras, two of which work in stereo for surveillance and tracking while the third zooms in for targeting. A digital video recorder captures data for up to 60 days at a time. By calling up the robot's ID number, operators back in Seoul can also see in real time what is happening in the field.

For use in the DMZ, the sentry bot doesn't need to distinguish friend from foe. "When you cross the line, you're automatically an enemy," Yoo says. He wouldn't say whether the robot has actually been deployed in the DMZ but did note that units are currently being assembled and tested at the company's factory in Changwon, near Pusan. Samsung is also looking to deploy the robot—minus the gun, but perhaps with some sort of nonlethal weapon—at airports, prisons, and nuclear power plants, among other places. There's no price tag as yet, but Yoo estimates it will be in the US $80 000 to $100 000 range.

By deploying the robots, Yoo thinks his government may be able to significantly reduce the mandatory two years of military service that all young Korean men now serve. His own son is a freshman in college and will soon be eligible for the army. "My son likes this robot," he says. **—JEAN KUMAGAI**

KIM DONG-JOO/AFP/GETTY IMAGES